(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 April 2002 (25.04.2002)

PCT

(10) International Publication Number
WO 02/033872 A3

(51) International Patent Classification[7]: G06F 17/60, H04L 9/00, 9/32

(21) International Application Number: PCT/US01/32590

(22) International Filing Date: 17 October 2001 (17.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/690.430 17 October 2000 (17.10.2000) US

(71) Applicants and
(72) Inventors: **KENNEDY, John, C.** [US/US]; 5548 N.W. 80th Terrace, Kansas City, MO 64151 (US). **AUSTAD, Melissa, Anne** [US/US]; 6135 W. 120th Street, #101, Overland Park, KS 66209 (US).

(74) Agent: **LUEBBERING, Thomas, B.**; Hovey, Williams, Timmons & Collins, Suite 400, 2405 Grand Boulevard, Kansas City, MO 64108 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

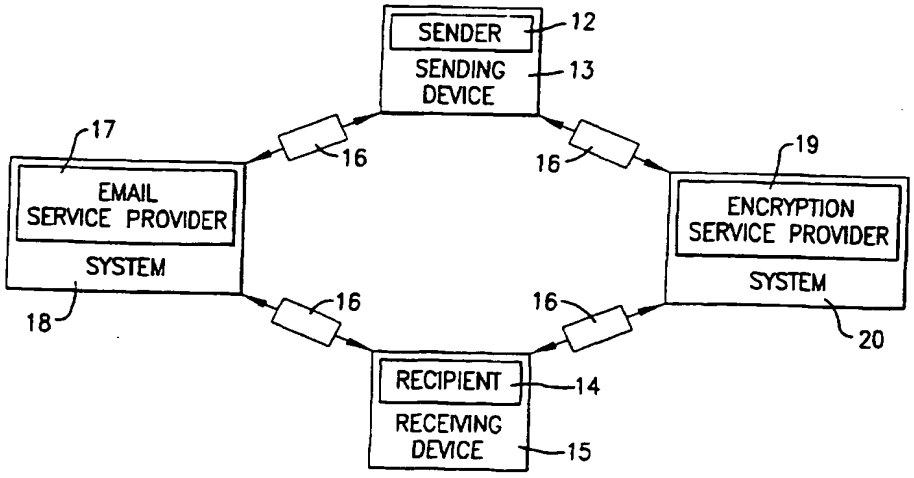
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
22 August 2002

[Continued on next page]

(54) Title: AN ELECTRONIC MESSAGE SERVICE PROVIDER SYSTEM, METHOD AND COMPUTER PROGRAM WITH CONFIGURABLE SECURITY SERVICE



(57) Abstract: A system (20), method, and computer program for providing a customizable e-message encryption scheme and service (19). The software or service may be purchased conventionally from a store or purchased online and downloaded (50). Upgrades and technical support are available online form the service provider (19, 52). Encryption algorithms of varying levels of complexity are available (57), and large customers can establish a security hierarchy dependent on context sensitivity and risk

02/033872 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/32590

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F/17/60;H04L/9/00,9/32
US CL : 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/201;705/26,27

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PROQUEST searched terms : outsource, security services, email, electronic mail, certified, united parcel

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	BLACKMAN, J. Secure E-Mail Law Office Computing, Dec 1998/Jan 1999, Vol 8, No 6 pages 85-87	1-7, 9-17,19-26,29,30 --- 8, 18
Y	SELWAY. MARK. Delivering the goods digitally:TECHNOLOGY ELECTRONIC COURIERS Finanancial Times; London. 23 June 1998 start page 15	8, 18
A	MICHAEL. T. TECHNOLOGY Delivering the goods online Financial Times; London. June 18, 1998, page 3	1-7, 10
A	US Postal Service Web site http://www.usps.com/shipping/eps_xtra.htm Copyright 1999-2000	1
Y, P	US 6,167,568 A (GANDEL et al) 26 December 2000 (26.12.2000), Abstract	1, 10, 20
Y	US 6,073,124 A (KRISHMAN et al) 06 June 2000 (06.06.2000), Abstract	1, 10, 20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 February 2002 (25.02.2002)

Date of mailing of the international search report
12 APR 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No.

Authorized officer
Gail Hayes
Peggy Harrod

Telephone No. 703-305-4276

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/32590

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6,014,651 A (CRAWFORD) 11 January 2000 (11.01.2000), Abstract	1, 10, 20
Y, E	US 6,324,569 B1 (OGILVIE et al) 27 November 2001 (27.11.2001), Abstract	1, 10, 20
A, T	United Parcel Service Web site http://www.exchange.ups.com/docs/ease.html Copyright 1994-2001	1
A, T	United Parcel Service Web site http://www.exchange.ups.com/docs/faq.html Copyright 1994-2002	1-7, 9-17, 19-26,29, 30
A, T	United Parcel Service Web site http://online.courier.ups.com/download/download.html Copyright 1994-2002	1
A, T	United Parcel Service Web site http://www.exchange.ups.com/docs/courier.html Copyright 1994-2000	1
A	UPS Online Courier Desktop Release Notes Readme.txt file December 1998	1, 10, 20
A	United Parcel Service. Getting Started with UPS OnLine Courier Desktop Document ver. 1.5 for Windows Operating System 1997	1-7, 9-17, 19-26, 29, 30

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/32590

Continuation of Item 4 of the first sheet:
AN ELECTRONIC MESSAGE SERVICE PROVIDER SYSTEM, METHOD AND COMPUTER PROGRAM WITH CONFIGURABLE SECURITY SERVICES

THIS PAGE BLANK (USPTO)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 April 2002 (25.04.2002)

PCT

(10) International Publication Number
WO 02/33872 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US01/32590

(22) International Filing Date: 17 October 2001 (17.10.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/690,430 17 October 2000 (17.10.2000) US

(71) Applicants and
(72) Inventors: **KENNEDY, John, C.** [US/US]; 5548 N.W. 80th Terrace, Kansas City, MO 64151 (US). **AUSTAD, Melissa, Anne** [US/US]; 6135 W. 120th Street, #101, Overland Park, KS 66209 (US).

(74) Agent: **LUEBBERING, Thomas, B.**; Hovey, Williams, Timmons & Collins, Suite 400, 2405 Grand Boulevard, Kansas City, MO 64108 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: A SYSTEM, METHOD, AND COMPUTER PROGRAM FOR ENCRYPTING E-MAIL

(57) Abstract: A system, method, and computer program for providing a customizable e-massage encryption scheme and service. The software or service may be purchased conventionally from a store or purchased online and downloaded. Upgrades and technical support are available online form the service provider. Encryption algorithms of varying levels of complexity are available, and large customers can establish a security hierarchy dependent on context sensitivity and risk exposure (e.g., destination, routing, firewall protection, etc.). Senders may use their existing e-message or e-mail provider, and encrypt while typing or when sending. Senders may also choose among several delivery and access options, including decryption options such that receivers need not themselves purchase the software or service in order to decode messages.

WO 02/33872 A2

A SYSTEM, METHOD, AND COMPUTER PROGRAM FOR ENCRYPTING E-MAIL

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention relates to systems, methods, and computer programs for encrypting electronic messages (e-messages) such as, for example, electronic mail (e-mail). More particularly, the invention relates to systems, methods, and computer programs for encrypting messages using techniques that are updateable, upgradeable, and customizable through on-line service providers.

2. DESCRIPTION OF THE PRIOR ART

It is often desirable to preserve security or personal privacy by encrypting e-messages, particularly e-mail, so that only those persons entrusted with the decryption or access key are able to view the message. Encryption techniques and software are well-known in the art, but suffer from several disadvantages. Encryption freeware or shareware, for example, though inexpensive, lacks technical support and can be notoriously cryptic and difficult for many consumers to use. Store-bought encryption software can suffer from the same lack of support, particularly where older or outdated versions of the software are involved. Though some providers do make patches and minor upgrades available for download via the Internet, major upgrades often require purchasing a new product.

Furthermore, although the security needs of the average consumer are very different from the security needs of a corporation, most encryption software and services do not provide for this level of customization, including varying degrees of security or use. That is, the average consumer may send e-messages relatively infrequently and need only occasional, minimally complex security measures. A corporation, however, may have hundreds or thousands of employees sending large amounts of e-messages requiring varying levels of security depending on such factors as content sensitivity, originating employee, and external exposure risk.

Also, encryption software that can only be conventionally purchased in a store is not immediately and conveniently available to an entity receiving an encrypted e-message and needing his or her own copy of the software to decode the message. Even where the software can be conveniently purchased and downloaded from an online service provider, it may not be practical to purchase every encryption program necessary to enable decoding all possible encryption formats and techniques.

Accordingly, there is a need for an improved, customizable system, method, and computer program operable to economically and efficiently encrypt and decrypt e-messages.

SUMMARY OF THE INVENTION

The present invention solves the above-described problems and provides a distinct advance in the art of scaleable, customizable e-message encryption schemes and services. More particularly, the present invention provides a system, method, and computer program that provides online purchasing and support options and customization based on such factors as security needs, security levels, and use.

In one preferred embodiment, a system for encrypting e-messages is provided that includes a sending device and a receiving device, one or more communications networks, and an encryption service provider. Though preferably embodied in personal computers, the sending and receiving devices may be virtually any electronic devices, including cellular telephones or electronic pagers, operable to send and receive, respectively, an electronic text message. Though preferably embodied in the Internet, the communications network may be any suitable communications network, including a local area network or wireless network. The encryption service provider is preferably an Internet-based website, though its nature may change to accommodate the various embodiments of other aspects of the present invention.

The operator of the sending device may obtain the service or software online or from a physical store. Upgrades and technical support are available online from the service provider. With regard to customization, the encryption service provider may provide encryption algorithms of varying levels of complexity, and large customers can establish a security hierarchy dependent on context sensitivity and risk exposure (e.g., destination,

routing, firewall protection, etc.). Senders operating the sending device may use their existing e-message or e-mail provider, and encrypt while typing or when sending. Senders may also choose among several delivery and access options so that receivers need not themselves purchase the software in order to decode messages.

These and other important aspects of the present invention are described more fully below in the section titled DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

A preferred embodiment of the present invention is described in detail below with reference to the attached drawing figures, wherein:

FIG. 1 is a computer-based system operable to implement a preferred embodiment of the present invention.

FIG. 2 is a flowchart illustrating certain steps in the method of a preferred embodiment of the present invention.

The drawing figures do not limit the present invention to the specific embodiments disclosed and described herein. The drawings are not necessarily to scale, emphasis instead being placed upon clearly illustrating the principles of the invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Referring to Fig. 1, a computer-based system 10 is illustrated constructed in accordance with a preferred embodiment of the present invention and operable to provide customizable e-message encryption capability. E-messages broadly include e-mail, instant messaging, and other suitable electronically-based messaging means and methods. The present invention can be implemented in hardware, software, firmware, or any combination thereof. In a preferred embodiment, however, the invention is implemented as a service provided via an Internet website that is hosted by and can be accessed with the computer equipment of the system 10, broadly comprising a Sender 12 operating an e-mail sending device 13; a Recipient 14 operating an e-mail receiving device 15; one or more communications networks 16; an e-mail service provider 17 operating an associated computer-based system 18; and an encryption service provider 19 operating an associated

computer-based system 20. The hardware and software illustrated and described herein are merely examples that may be used to implement the present invention but that may be replaced with other hardware or software performing equivalent functions without departing from the scope of the present invention.

The sending device 13, receiving device 15, and the service provider systems 18,20 all include hardware and software operable to send and receive e-mail. The Sender 12 operating the sending device 13 may be, for example, a private individual or one of hundreds of employees of a corporate client. The sending device 13 preferably comprises a personal computer, such as those manufactured and sold by Dell, Compaq, Gateway, or any other computer manufacturer. Alternatively, the sending device 13 may comprise any type of device that permits access to the encryption or e-mail service providers' systems 18,20 via the communications network 16, including personal computers, handheld personal assistants such as those manufactured and sold by Palm or Pilot, or even application specific appliances designed almost exclusively for e-mailing or accessing the communications network 16. Whatever its nature, the sending device 13 preferably further includes or can access a conventional Internet connection such as a modem, DSL converter, or ISDN converter and a web browser that permits it to access and navigate the communications network 16.

The Recipient 14 may also be, for example, a private individual or one of hundreds of employees of a corporation. The receiving device 15 preferably comprises a personal computer similar to the sending device 13, though may alternatively comprise any device with the requisite send/receive e-mail capability, including a cellular telephone or electronic pager.

The e-mail service provider 17 may be a single entity to which both Sender 12 and Recipient 14 are subscribers, or multiple separate entities between which email originating with the Sender 12 for delivery to the Recipient 14 is communicated. Numerous such e-mail service providers 17 exist, and no particular one is required by the present invention.

The network 16 electronically links and allows for the communication of e-mail between the sending device 13, service provider systems 18,20, and the receiving device 15. The network 16 is preferably the Internet but may be any communications network

operable to provide the requisite electronic link, such as a local area network, a wide area network, a wireless network, or an intranet, or any combination thereof.

The encryption service provider 19 uses the computer-based system 20 to provide customizable encryption services to its clients and subscribers, which in the present description are embodied in the Sender 12. The encryption service provider's system 20 comprises a host computer (not separately shown) to operate or host the provider's Internet website and serve as a repository for data and programs used to implement certain aspects of the present invention, as described in more detail below. The host computer may be any computing device such as a network computer running Windows NT, Novell Netware, Unix, or any other network operating system. The host computer may include a firewall or other security measures to prevent tampering with information stored on or accessible by the host computer. The host computer includes conventional web hosting operating software, and a connection for accessing the computer network 16, such as a modem, DSL converter or ISDN converter. In Internet contexts, the encryption service provider's system 20 is assigned a uniform resource locator (URL) and corresponding domain name such as "customencryption.com" so that the website hosted thereon can be accessed via the Internet in a conventional manner.

The one or more computer programs used to implement the present invention are stored in or on computer-readable medium residing on or accessible by the host computer, and are operable to instruct the host computer in operating the encryption service provider's website as described herein. The computer programs preferably comprise ordered listings of executable instructions for implementing logical functions in the host computer and other computing devices coupled with the host computer.

The computer programs may be embodied in any computer-readable medium for use by or in connection with an instruction execution system, apparatus, or device, such as the preferred computer-based system, a processor-containing system, or any other system that can fetch the instructions from the instruction execution system, apparatus, or device, and execute the instructions. In the context of this application, a "computer-readable medium" can be any means that can contain, store, communicate, propagate or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer-readable medium can be, for example, but is not

limited to, an electronic, magnetic, optical, electro-magnetic, infrared, or semi-conductor system, apparatus, device, or propagation medium. More specific, although not inclusive, examples of the computer-readable medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a random access memory (RAM), a read-only memory (ROM), an erasable, programmable, read-only memory (EPROM or Flash memory), an optical fiber, and a portable compact disk read-only memory (CDROM). The computer-readable medium could even be paper, for example, or another suitable medium upon which the program is printed, as the program can be electronically captured, via for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory.

The computer programs includes code segments for encrypting the Sender's e-mail. In general, there are several well-known methods for encrypting information, including key tables, simple formulas, and algorithms. The present invention uses updateable algorithms or formulas that lend themselves to reformulation. That is, as the encryption software is periodically updated such that the actual code of encryption may change, thereby foiling ongoing attempts to crack a stagnant code.

The encryption service provider 19 is able to use the system 20 to make the encryption software available for convenient online purchase and download. Tutorials and support services are identical regardless of whether the software was purchased conventionally from a store or downloaded from the service provider's website. The Sender 12 is preferably required to register with the encryption service provider's system 20, which provides a database for announcing upgrades and other relevant product/service messages.

The flow chart of Fig. 2 shows in more detail the functionality and operation of a preferred implementation of the present invention. In this regard, the boxes of the flow chart may represent a module segment or portion of code of the computer programs of the present invention which comprises one or more executable instructions for implementing the specified logical function or functions. In some alternative implementations, the functions noted in the various blocks may occur out of the order depicted in Fig. 2. For example, two blocks shown in succession in Fig. 2 may in fact be executed substantially

concurrently, or the blocks may sometimes be executed in the reverse order depending upon the functionality involved.

In operation, the Sender 12, desiring to send and prevent unauthorized persons from accessing and reading personal e-mail, either purchases the encryption software of the present invention conventionally or pays for and downloads it from the encryption service provider 19 via the Internet 16, as is depicted by box 50. Alternatively, if the sender's e-mail service provider 17 supports doing so, the Sender 12 may be able to encrypt each e-mail on a per-use basis without purchasing the software. After purchasing and installing the software, the Sender 12 preferably accesses the encryption service provider's website and registers their ownership, as is depicted by box 52.

Alternatively, the Sender 12 may have a per-use option not requiring purchase of the encryption software. In this form, the Sender 12 is able to encrypt particularly sensitive e-mails as desired on a per-use payment basis, preferably using an activateable icon appearing on the e-mail webpage provided by the e-mail service provider 17. This presumably would require an agreement between the encryption service provider 19 and the e-mail service provider 17.

Corporate or other clients requiring higher levels of security or customization may contact the encryption service provider directly and arrange for a carefully tailored e-mail security scheme, which may, for example, include unique encryption algorithms. Depending on the client's size, an independent encryption server (not shown) may be required to handle the traffic. Preferably, such a server would be serviced only by the encryption service provider 19 as any attempt by the client to access or tamper with the encryption source code would disable the software and send e-mails warning of the attempt, as described below.

For corporate clients, single- and multi-tiered security schemes may be provided. In a first form, all licensed users of a single client would have the same encryption software and the same security level. This is useful where the only purpose of encryption is to prevent outsiders from accessing internal messages. In a second form, the employees of a single corporate client, for example, would be divided into several tiers, each representing a different security level, and each such security level would have its own encryption software. Each employee's ability to protect their own e-mail and their ability to

decrypt others' e-mail can be based on whatever factors are deemed relevant, including the employee's position, department, trustworthiness, or need-to-know. Preferably, each employee would be able to decrypt e-mails encrypted at the same or lower encryption/security level. This allows supervisors, for example, to monitor their staff's e-mails, while protecting executive's e-mails from being accessed by lower level employees. In a third form, several different encryption formulas are put in place without regard to employee security level. This ensures that all e-mails will be unreadable except by those to whom it was intended.

When desiring to send an encrypted e-mail, the Sender 12 accesses its e-mail service provider's system 18, and decides whether to enable encryption while typing or to encrypt when finished, as is depicted by box 54. The present invention, however, in no way interferes with the Sender's ability to send non-encrypted e-mail unless such a limitation is a part of the customized service. The message is then typed or otherwise entered or prepared for sending, as is depicted by box 56.

Prior to sending, the Sender 12 is prompted to specify a delivery method, whether the originating and terminating addresses should be encrypted, and whether to be notified if an unintended recipient attempts to open or decrypt the message, as is depicted by box 57. The Sender 12 also has the option of encrypting its and the Recipient's e-mail addresses as well. By exercising this last option, only the system administrator of the encryption service provider 19 would be able to trace the Sender 12 or Recipient 14. Defaults may be established such that thereafter these decisions only need be made when desiring an option other than the default. The e-mail is then sent, as is depicted by box 58.

Additional options, particularly for corporate clients, include automatically encrypting all e-mail, or automatically encrypting some e-mail based on a pre-established criteria. For example, a corporation may desire automatic encryption for all e-mail originating internally and having an external destination. In another option, all internally encrypted e-mail would have an identifying header, thereby allowing the system administrator to identify externally originating encrypted e-mail.

The Sender 12 preferably may choose one of three or more various delivery and decryption or access methods. In a first form, the Sender 12 can require that the Recipient 14 have the same encryption software and the same version/format as the

Sender 12 in order to decrypt the message. If the Recipient 14 does not, he will be required to purchase the software or update his existing version prior to accessing the e-mail. In a second form, the Sender 12 could simply password-enable the message, thereby not requiring that the Recipient 14 have the same encryption software. The password alone allows the Recipient 14 to decrypt the e-mail. In a third form, the Sender 12 can send the e-mail to a specified address within the encryption service provider's site. The service provider 19 then sends an e-mail to the intended Recipient 14 alerting it that a message is being held. The Recipient 14 would be required to prove its identity, possibly by passing a test, such as correctly answering a series of three or four Sender-supplied questions, in order to gain access to the decrypted message. If the Recipient 14 fails the test, for example, by giving an incorrect answer, then the e-mail is preferably deleted and the Sender 12 notified of the failure to deliver. This last form of delivery does not require that the Recipient 14 have the same encryption software as the Sender 12.

All of the above described client packages can use any or all of the above described delivery methods. Even where a client uses its own dedicated server, messages can be sent to the encryption service provider 19 for subsequent retrieval by the intended Recipient 14.

The path taken by the encrypted e-mail will depend on the delivery and access method specified. In any event, the e-mail will first travel via the e-mail service provider 17, as depicted by box 60. From there, intermediate delivery may be to the encryption service provider 19 such that the Recipient 14 must thereafter contact the provider 19 and satisfy certain access requirements, which are described above, as is depicted by box 62. Otherwise, the encrypted e-mail will proceed directly to the Recipient 14, as depicted by box 64.

It is further contemplated that any unauthorized attempt at any point in the encryption process to breach the source code of the encryption software will cause a warning e-mail to be sent to the encryption service provider 19 regarding the attempt, as depicted by box 66. This feature is included to prevent parties from "reverse engineering" the program code to discover means to defeat the encryption. Preferably, even the Sender 12 itself is not authorized to access the source code, regardless of whether it has purchased the actual software, and any attempt to do so will disable the encryption software

and also cause a warning e-mail to be sent to the encryption service provider 15 regarding the attempt.

Although the invention has been described with reference to the preferred embodiment illustrated in the attached drawing figures, it is noted that equivalents may be employed and substitutions made herein without departing from the scope of the invention as recited in the claims. For example, the sending device 12 may comprise a type of cellular telephone having a display and being operable to send the encrypted e-message via an ordinary wireless communication network 16 to the Recipient's cellular telephone, or to the encryption service provider 19 whom the Recipient 14 must then call, possibly using a toll-free number, to retrieve the e-message. This example embodiment may not require an e-message or e-mail service provider 17.

Having thus described the preferred embodiment of the invention, what is claimed as new and desired to be protected by Letters Patent includes the following:

CLAIMS:

1. An encryption service provider for encrypting an electronic message, the encryption service provider being operable to:

send and receive an electronic message via a communications network;

provide encryption software for download via the communications network to a sending device;

receive an encrypted electronic message from the sending device, the sending device specifying a form of delivery, a form of access, and a recipient;

require the recipient to satisfy the form of access in order to access the encrypted electronic message; and

satisfy the form of delivery if the recipient has satisfied the form of access.

2. The encryption service provider of claim 1, the encrypted electronic message being in one of the following forms: electronic mail, instant messaging.

3. The encryption service provider of claim 1, the sending device being one of the following: a personal computer, a cellular telephone, a pager, a handheld computing device.

4. The encryption service provider of claim 1, the communication network being one of the following: the Internet, a local area network, a wireless network.

5. The encryption service provider of claim 1, the form of delivery being direct delivery of the encrypted electronic message to the recipient.

6. The encryption service provider of claim 1, the form of delivery being intermediate delivery of the encrypted electronic message to the encryption service provider, and subsequent delivery of the encrypted electronic message from the encryption service provider to the recipient upon satisfaction of the form of access.

7. The encryption service provider of claim 6, the form of access being satisfied by the recipient providing at least one correct answer to at least one question.

8. The encryption service provider of claim 1, the encryption service provider being further operable to provide a warning that an attempt has been made to deliver the encrypted electronic message without satisfying the specified form of delivery.

9. The encryption service provider of claim 1, the encryption service provider being further operable to provide a warning that an attempt has been made to access the encrypted electronic message without satisfying the specified form of access.

10. A method for encrypting an electronic message intended for delivery to and access by a designated recipient, the method comprising the steps of:

(a) allowing a sender to access software operable to encrypt the electronic message;

(b) allowing the sender to specify a form of delivery;

(c) allowing the sender to specify a form of access;

(d) allowing the encrypted electronic message to be delivered in accordance with the specified form of delivery; and

(f) allowing the encrypted electronic message to be accessed by a recipient in accordance with the specified form of access.

11. The method as set forth in claim 10, the encrypted electronic message being in one of the following forms: electronic mail, instant messaging.

12. The method as set forth in claim 10, step (a) being accomplished by providing one or more computer-readable memory devices containing the software.

13. The method as set forth in claim 10, step (a) being accomplished by providing the software for download via a communications network.

14. The method as set forth in claim 10, the specified form of delivery being direct delivery of the encrypted electronic message to the designated recipient having software operable to decrypt the encrypted electronic message.

15. The method as set forth in claim 10, the specified form of delivery being direct delivery of the encrypted electronic message to the designated recipient, the specified form of access requiring provision of at least one correct password.

16. The method as set forth in claim 10, the specified form of delivery being delivery of the encrypted electronic message to a third-party, the third-party communicating to the designated recipient that the electronic message has been delivered to the third-party and requesting that the designated recipient contact the third-party in order to satisfy the specified form of access.

17. The method as set forth in claim 16, the specified form of access to the electronic mail being the provision of one or more correct answers to one or more questions.

18. The method as set forth in claim 10, further including the step of (g) communicating a warning message if delivery of the encrypted electronic message is attempted in a form not in accordance with the specified form of delivery.

19. The method as set forth in claim 10, further including the step of (g) communicating a warning message if access to the encrypted electronic message is attempted in a form not in accordance with the specified form of access.

20. A method for providing customizable encryption services for encrypting an electronic message intended for delivery to and access by a designated recipient, the method comprising the steps of:

(a) providing software operable to encrypt and decrypt the electronic message using one or more encryption algorithms;

(b) providing an amount of technical support for the software, the technical support including assistance in operating the software;

(c) providing an amount of assistance in the delivery to and access by the designated recipient of the encrypted electronic message; and

(d) charging a fee for the encryption service, the fee being based on criteria such as the number of encryption algorithms used, the amount of technical support provided, the amount of assistance provided in the delivery to and access by the designated recipient.

21. The method as set forth in claim 20, the encrypted electronic message being in one of the following forms: electronic mail, instant messaging.

22. The method as set forth in claim 20, step (a) being accomplished by providing one or more computer-readable memory devices containing the software.

23. The method as set forth in claim 20, step (a) being accomplished by allowing the software to be received via a communications network by an electronic device.

24. The method as set forth in claim 20, step (c) being accomplished by acting as an intermediate recipient from which the designated recipient may access the electronic message by satisfying at least one pre-established access condition.

25. The method as set forth in claim 24, the pre-established access condition being provision of at least one correct answer to at least one question.

26. The method as set forth in claim 20, step (d) being accomplished on a per use basis with a fee being charged for each use of the encryption services.

27. The method as set forth in claim 20, the method further comprising the step of (e) establishing a security hierarchy based on pre-established criteria, the security hierarchy comprising a plurality of hierarchical security levels, each security level having its own encryption algorithm for encrypting the electronic message and being able to decrypt the electronic message encrypted using the same algorithm.

28. The method as set forth in claim 27, each security level being able to access and decrypt the electronic message of all of the security levels lower in the hierarchy, and each security level being unable to access and decrypt the electronic message of all of the security level higher in the hierarchy.

29. A combination of computer code segments, each computer code segment being stored on a computer-readable memory, the combination of computer code segments being operable to facilitate the encryption of an electronic message intended for delivery to and access by a designated recipient, the combination of computer code segments comprising:

a program code segment operable to allow for electronic communications via a communications network;

a program code segment operable to encrypt the electronic message;

a program code segment operable to receive input specifying a form of delivery and to allow for the delivery of the encrypted electronic message in accordance with the specified form of delivery;

a program code segment operable to receive input specifying a form of access and to allow for the delivery of the encrypted electronic message in accordance with the specified form of access; and

a program code segment operable to decrypt the encrypted electronic message.

30. The computer program set forth in claim 29, the program code segment operable to encrypt the electronic message by selecting an encryption algorithm from a set of possible encryption algorithms.

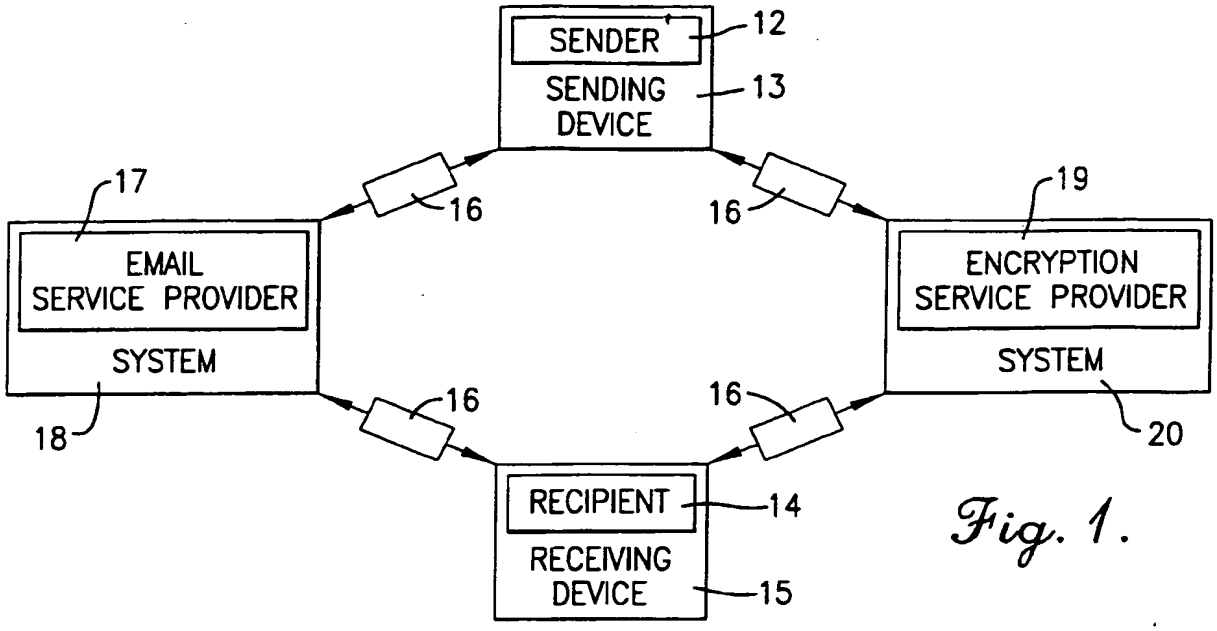

SENDER
12
SENDING DEVICE
13
16
16
17
EMAIL SERVICE PROVIDER
SYSTEM
18
19
ENCRYPTION SERVICE PROVIDER
SYSTEM
20
16
16
RECIPIENT
14
RECEIVING DEVICE
15

Fig. 1.

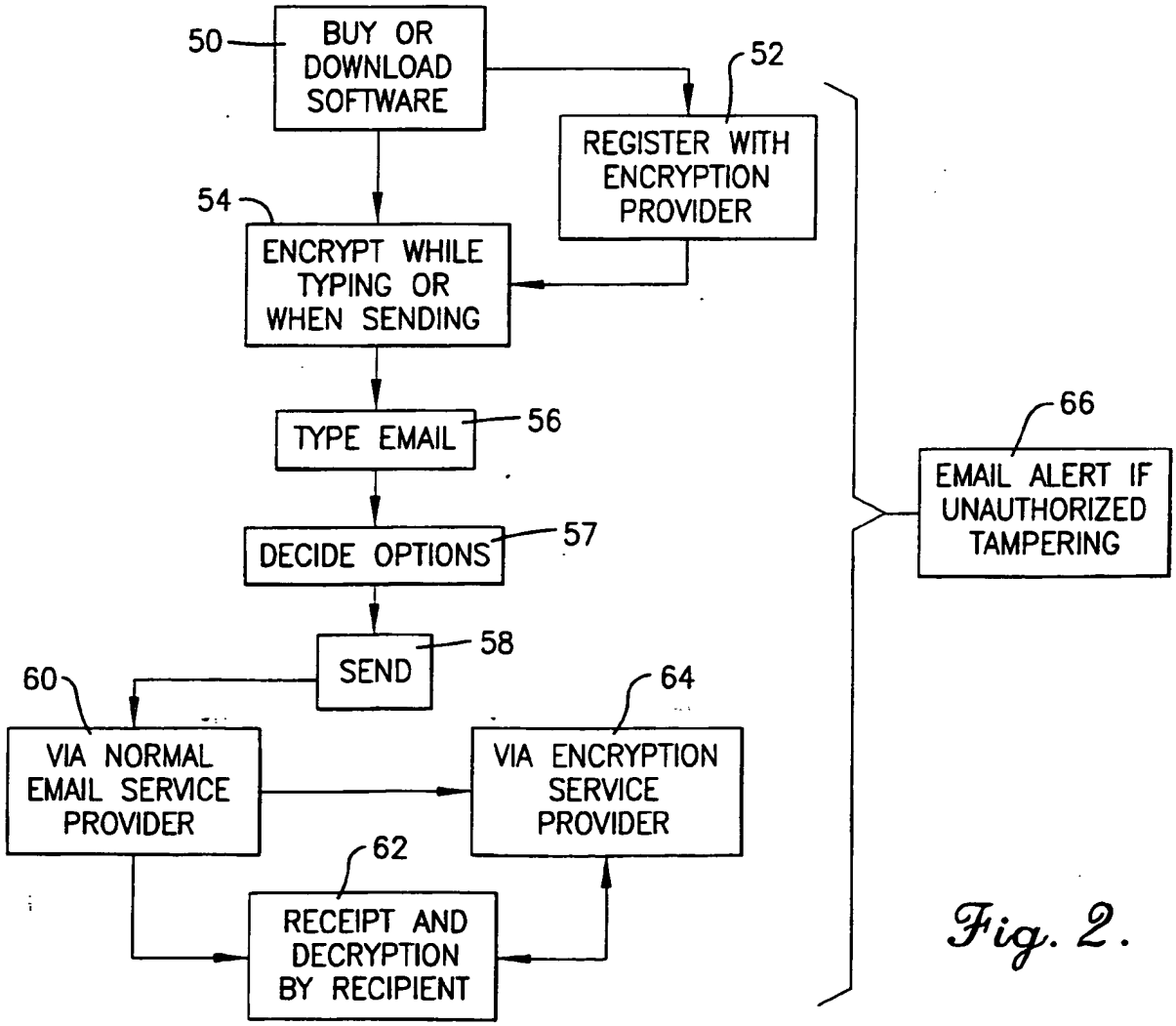

50
BUY OR DOWNLOAD SOFTWARE
52
REGISTER WITH ENCRYPTION PROVIDER
54
ENCRYPT WHILE TYPING OR WHEN SENDING
TYPE EMAIL
56
DECIDE OPTIONS
57
SEND
58
60
VIA NORMAL EMAIL SERVICE PROVIDER
64
VIA ENCRYPTION SERVICE PROVIDER
62
RECEIPT AND DECRYPTION BY RECIPIENT
66
EMAIL ALERT IF UNAUTHORIZED TAMPERING

Fig. 2.

THIS PAGE BLANK (USPTO)